## **Unit 11 Submission File: Network Security Homework**

### **Part 1: Review Questions**

#### **Security Control Types**

The concept of defense in depth can be broken down into three different security control types. Identify the security control type of each set of defense tactics.

1. Walls, bollards, fences, guard dogs, cameras, and lighting are what type of security control?  
     
    Answer: Physical Controls
2. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?  
     
    Answer: Administrative Controls
3. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?  
     
    Answer: Technical Controls

#### **Intrusion Detection and Attack indicators**

1. What's the difference between an IDS and an IPS?  
     
    Answer:

|  |  |
| --- | --- |
| IDS | IPS |
| Detection and alerts of an attack | Provides controls to deny attacks |
| Passive (they do not respond to attack, they log and document information) | Active (can reject packets based on rules) |
| Used to establish situational awareness of attackers allowing them to harnden defenses | May be used to quickly shut down the damage and protect overall network |
| IDS connects via Network TAP or Mirrored SPAN port; typically placed next router or switch | IPS connects in-line with flow of data typically between firewall and network switch |

1. What's the difference between an Indicator of Attack and an Indicator of Compromise?  
     
    Answer: Indicator of Compromise is an indicator that a network has been breached and is usually gathered after being informed of suspicious activity. This is a reactive approach. They cannot detect zero-day exploits.

Indicator of Attack is an indicator that focuses on detecting the intent of the attacker and what they are trying to accomplish. IOA involves observing for behaviors of the attacker as they execute. This is a real-time approach and may be used to detect zero-day exploits.

#### **The Cyber Kill Chain**

Name each of the seven stages for the Cyber Kill chain and provide a brief example of each.

1. Stage 1: Reconnaissance : Attackers probe for a weakness like harvesting login credentials or information useful for a phishing attack like finding email addresses of recipients.
2. Stage 2: Weaponization : Build a deliverable Payload using the exploit from Reconnaissance. Example: compile the phishing email to be delivered.
3. Stage 3: Delivery : Sending the weaponised bundle to the victim. Example: delivering the email with malicious links in a legitimate looking email.
4. Stage 4: Exploitation : Executing code on victim’s system. Example: When the user clicks on the malicious link, download the code on the victim's system.
5. Stage 5:Installation : Installing malware on the target asset. Example: Installing the code downloaded in Stage 4.
6. Stage 6: Command and Control : Creating a channel where the attacker can control the system remotely. Example: Send a message to the command center that the victim’s system has been compromised successfully and to send instructions.
7. Stage 7: Actions on Objective : Attacker remotely carries out its intended goal. Example : Instructions sent from the Command center to send emails to people in the victim's address book asking for money.

#### **Snort Rule Analysis**

Use the Snort rule to answer the following questions:

Snort Rule #1

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by\_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5; metadata:created\_at 2010\_07\_30, updated\_at 2010\_07\_30;)

1. Break down the Sort Rule header and explain what is happening.  
     
    Answer: Rule header is

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5800:5820

The rule is to alert on tcp protocol for packets from “$External\_Net” (Internet) source and any source port to “$HOME\_NET” (home network) destination on destination ports ranging from 5800 to 5820.

1. What stage of the Cyber Kill Chain does this alert violate?  
     
    Answer: Reconnaissance. The attacker is attempting to probe for a weakness on ports 5800 through 5820 for VNC (Virtual Network Computing) service exploit from an external untrusted network.
2. What kind of attack is indicated?  
     
    Answer: This is a Port Scan Attack since the attacker is scanning to identify if ports 5800 through 5820 are open for a potential VNC exploit.

Snort Rule #2

alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; flow:established,to\_client; flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file\_data; content:"MZ"; within:2; byte\_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata: former\_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Main/2018959; classtype:policy-violation; sid:2018959; rev:4; metadata:created\_at 2014\_08\_19, updated\_at 2017\_02\_01;)

1. Break down the Sort Rule header and explain what is happening.  
     
    Answer: Rule Header is

alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any

The rule is to alert on tcp protocol for packets from source $EXTERNAL\_NET (Internet) source and source port $HTTP\_PORTS to “$HOME\_NET” (home network) destination on any destination port. It alerts if a user is trying to download a file (which uses TCP) from a website that runs on Http Port (80 or whatever the variable value $HTTP\_PORTS is set to).

1. What layer of the Defense in Depth model does this alert violate?  
     
    Answer: This alert works on the Network Security Controls layer (Technical Controls) of Defence in Depth model since this alert is part of an IDS.
2. What kind of attack is indicated?  
     
    Answer: This could be a Drive by Download attack where the victim is accessing an unsecure website running on port 80 which would download the payload automatically without asking for the user’s permission.

Snort Rule #3

* Your turn! Write a Snort rule that alerts when traffic is detected inbound on port 4444 to the local network on any port. Be sure to include the msg in the Rule Option.  
    
   Answer:  
  alert ip any 4444 -> “$HOME\_NET” any {msg: "IP Packet Detected on local network from port 4444";}

### **Part 2: "Drop Zone" Lab**

#### **Log into the Azure firewalld machine**

Log in using the following credentials:

* Username: sysadmin
* Password: cybersecurity

#### **Uninstall ufw**

Before getting started, you should verify that you do not have any instances of ufw running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

* Run the command that removes any running instance of ufw.  
    
   $ sudo apt remove ufw -y

#### **Enable and start firewalld**

By default, these service should be running. If not, then run the following commands:

Run the commands that enable and start firewalld upon boots and reboots.  
  
 $ sudo systemctl enable firewalld

* $ service firewalld start
* $ sudo /etc/init.d/firewalld start  
    
   Note: This will ensure that firewalld remains active after each reboot.

#### **Confirm that the service is running.**

* Run the command that checks whether or not the firewalld service is up and running.  
    
   $ service firewalld status

#### **List all firewall rules currently configured.**

Next, lists all currently configured firewall rules. This will give you a good idea of what's currently configured and save you time in the long run by not doing double work.

* Run the command that lists all currently configured firewall rules:  
    
   $ sudo firewall-cmd --list-all-zones
* Take note of what Zones and settings are configured. You many need to remove unneeded services and settings.

#### **List all supported service types that can be enabled.**

* Run the command that lists all currently supported services to see if the service you need is available  
    
   $ sudo firewall-cmd --get-services
* We can see that the Home and Drop Zones are created by default.

#### **Zone Views**

* Run the command that lists all currently configured zones.  
    
   $ sudo firewall-cmd --get-zones
* We can see that the Public and Drop Zones are created by default. Therefore, we will need to create Zones for Web, Sales, and Mail.

#### **Create Zones for Web, Sales and Mail.**

Run the commands that creates Web, Sales and Mail zones.  
  
 $ sudo firewall-cmd --new-zone=Web --permanent

$ sudo firewall-cmd --new-zone=Sales --permanent

$ sudo firewall-cmd --new-zone=Mail --permanent

#### **Set the zones to their designated interfaces:**

Run the command that sets your eth0 interface to your zones.  
  
 $ sudo firewall-cmd --zone=Web --change-interface=eth0

$ sudo firewall-cmd --zone=Sales --change-interface=eth0

$ sudo firewall-cmd --zone=Mail --change-interface=eth0

* $ service firewalld restart
* $ firewall-cmd --runtime-to-permanent

#### **Add services to the active zones:**

* Run the commands that add services to the **public** zone, the **web** zone, the **sales** zone, and the **mail** zone.
* Public:  
    
  $ sudo firewall-cmd --zone=public --add-service=http

$ sudo firewall-cmd --zone=public --add-service=https

$ sudo firewall-cmd --zone=public --add-service=pop3

$ sudo firewall-cmd --zone=public --add-service=smtp

$ sudo firewall-cmd --zone=public --change-interface=eth0

* Web:  
    
   $ sudo firewall-cmd --zone=Web --add-source=201.45.34.126

$ sudo firewall-cmd --zone=Web --add-service=http

$ sudo firewall-cmd --zone=Web --change-interface=eth1

* Sales  
    
   $ sudo firewall-cmd --zone=Sales --add-source=201.45.15.48

$ sudo firewall-cmd --zone=Sales --add-service=https

$ sudo firewall-cmd --zone=Sales --change-interface=eth2

* Mail  
    
   $ sudo firewall-cmd --zone=Mail --add-source=201.45.105.12

$ sudo firewall-cmd --zone=Mail --add-service=smtp

$ sudo firewall-cmd --zone=Mail --add-service=pop3

$ sudo firewall-cmd --zone=Mail --change-interface=eth3

* What is the status of http, https, smtp and pop3?

#### **Add your adversaries to the Drop Zone.**

Run the command that will add all current and any future blacklisted IPs to the Drop Zone.  
  
 $ sudo firewall-cmd --zone=drop --add-source=10.208.56.23

$ sudo firewall-cmd --zone=drop --add-source=135.95.103.76

$ sudo firewall-cmd --zone=drop --add-source=76.34.169.118

#### **Make rules permanent then reload them:**

It's good practice to ensure that your firewalld installation remains nailed up and retains its services across reboots. This ensure that the network remains secured after unplanned outages such as power failures.

* Run the command that reloads the firewalld configurations and writes it to memory  
    
   $ sudo firewall-cmd --runtime-to-permanent

$ sudo firewall-cmd --reload

#### **View active Zones**

Now, we'll want to provide truncated listings of all currently **active** zones. This a good time to verify your zone settings.

* Run the command that displays all zone services.  
    
   $ sudo firewall-cmd --get-active-zones

$ sudo firewall-cmd --zone=drop --list-all

$ sudo firewall-cmd --zone=public --list-all

$ sudo firewall-cmd --zone=Mail --list-all

$ sudo firewall-cmd --zone=Sales --list-all

$ sudo firewall-cmd --zone=Web --list-all

#### **Block an IP address**

* Use a rich-rule that blocks the IP address 138.138.0.3.  
    
   $ sudo firewall-cmd --add-rich-rule="rule family='ipv4' source address='138.138.0.3' reject"

#### **Block Ping/ICMP Requests**

Harden your network against ping scans by blocking icmp echo replies.

* Run the command that blocks pings and icmp requests in your public zone.  
    
   $ sudo firewall-cmd --zone=public --add-icmp-block-inversion --permanent

$ sudo firewall-cmd --reload

#### **Rule Check**

Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.

Run the command that lists all of the rule settings. Do one command at a time for each zone.  
  
 $ sudo firewall-cmd --zone=drop --list-all

$ sudo firewall-cmd --zone=public --list-all

$ sudo firewall-cmd --zone=Mail --list-all

$ sudo firewall-cmd --zone=Sales --list-all

$ sudo firewall-cmd --zone=Web --list-all

* Are all of our rules in place? If not, then go back and make the necessary modifications before checking again.

Congratulations! You have successfully configured and deployed a fully comprehensive firewalld installation.

### **Part 3: IDS, IPS, DiD and Firewalls**

Now, we will work on another lab. Before you start, complete the following review questions.

#### **IDS vs. IPS Systems**

1. Name and define two ways an IDS connects to a network.  
     
    Answer 1: Network TAP (Test Access Port) is a hardware device that provides access to a network. It taps both inbound and outbound traffic data streams on separate channels at the same time.  
     
    Answer 2: SPAN (Switched Port Analyzer) sends a mirror image of all network data to another physical port where the packets are captured and analyzed.
2. Describe how an IPS connects to a network.  
     
    Answer: IPS connects in-line with flow of data. It typically sits between the firewall and network switch. It requires a robust hardware because all traffic flows through IPS and is evaluated against the rules which determine if it should be blocked or allowed.
3. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect Zero-Day attacks?  
     
    Answer: Signature-based IDS
4. Which type of IDS is beneficial for detecting all suspicious traffic that deviates from the well-known baseline and is excellent at detecting when an attacker probes or sweeps a network?  
     
    Answer: Anomaly-based IDS

#### **Defense in Depth**

1. For each of the following scenarios, provide the layer of Defense in Depth that applies:  
   1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.  
        
       Answer: Perimeter layer (Physical control); apply controls on tailgating like turnstiles
   2. A zero-day goes undetected by antivirus software.  
        
       Answer: Application layer (Technical Control); apply IOA solutions and get feeds from providers like carbonblack that provide zero-day vulnerability feeds
   3. A criminal successfully gains access to HR’s database.  
        
       Answer: Application and Data layer (Technical Control); This is IOC since the criminal has access already; Look for data integrity and exfiltration
   4. A criminal hacker exploits a vulnerability within an operating system.  
        
       Answer: Host and Application layer (Technical Control); Keep OS up to date with patches
   5. A hacktivist organization successfully performs a DDoS attack, taking down a government website.  
        
       Answer: Network Layer (Technical Control); Create firewall rules like rate limiting to avoid DDoS
   6. Data is classified at the wrong classification level.  
        
       Answer: Data Layer (Administrative Control); Start a project to analyze data in all systems across the company and classify them accordingly.
   7. A state sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.  
        
       Answer: Network Layer (Technical Control); Block ICMP Time Exceeded messages
2. Name one method of protecting data-at-rest from being readable on hard drive.  
     
    Answer: Disk encryption
3. Name one method to protect data-in-transit.  
     
    Answer: Always use secure websites (HTTPS); Do not connect to Public Wi-fi networks; Use VPN
4. What technology could provide law enforcement with the ability to track and recover a stolen laptop.  
     
    Answer: GPS and Wifi geolocation coupled with MacAddress; Find my Mac and find my device feature for Windows
5. How could you prevent an attacker from booting a stolen laptop using an external hard drive?  
     
    Answer: Put a password on BIOS config and disable booting from external media in BIOS configuration. (BIOS password can be reset by removing laptop battery and the CMOS battery though)

#### **Firewall Architectures and Methodologies**

1. Which type of firewall verifies the three-way TCP handshake? TCP handshake checks are designed to ensure that session packets are from legitimate sources.

Answer: Circuit Level Firewalls

1. Which type of firewall considers the connection as a whole? Meaning, instead of looking at only individual packets, these firewalls look at whole streams of packets at one time.

Answer: Packet-filtering Firewalls (Stateful)

1. Which type of firewall intercepts all traffic prior to being forwarded to its final destination. In a sense, these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it?

Answer: Application (Proxy) Firewalls

1. Which type of firewall examines data within a packet as it progresses through a network interface by examining source and destination IP address, port number, and packet type- all without opening the packet to inspect its contents?

Answer: Packet-filtering Firewalls (Stateless)

1. Which type of firewall filters based solely on source and destination MAC address?

Answer: Mac Layer Firewall

### **Bonus Lab: "Green Eggs & SPAM"**

In this activity, you will target spam, uncover its whereabouts, and attempt to discover the intent of the attacker.

* You will assume the role of a Jr. Security administrator working for the Department of Technology for the State of California.
* As a junior administrator, your primary role is to perform the initial triage of alert data: the initial investigation and analysis followed by an escalation of high priority alerts to senior incident handlers for further review.
* You will work as part of a Computer and Incident Response Team (CIRT), responsible for compiling **Threat Intelligence** as part of your incident report.

#### **Threat Intelligence Card**

**Note**: Log into the Security Onion VM and use the following **Indicator of Attack** to complete this portion of the homework.

Locate the following Indicator of Attack in Sguil based off of the following:

* **Source IP/Port**: 188.124.9.56:80
* **Destination Address/Port**: 192.168.3.35:1035
* **Event Message**: ET TROJAN JS/Nemucod.M.gen downloading EXE payload

Answer the following:

1. What was the indicator of an attack?  
   * Hint: What do the details of the reveal?

Answer: There was a download from an unsecure website (Port 80).

1. What was the adversarial motivation (purpose of attack)?  
     
    Answer: The purpose of the attack was to install malware called Gozi stealer without being detected by the user. The malware is used to exfiltrate sensitive data of victim to the attacker.
2. Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table.

|  |  |  |
| --- | --- | --- |
| **TTP** | **Example** | **Findings** |
| **Reconnaissance** | How did the attacker locate the victim? | Attacker would send emails to recipients in mass mailings and are usually socially engineered to appear enticing |
| **Weaponization** | What was it that was downloaded? | TROJAN JS/Nemucod.M.gen |
| **Delivery** | How was it downloaded? | TROJAN JS/Nemucod.M.gen was embedded in zip file which is an attachment in the email |
| **Exploitation** | What does the exploit do? | The exploit would download a file and run it to download malwares |
| **Installation** | How is the exploit installed? | The exploit is installed when user opens the email and clicks on/opens javascript file in the attachment |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | The downloaded file installs other malwares which then execute on the system. The computer is then restarted and Gozi malware starts phoning command server |
| **Actions on Objectives** | What does the software that the attacker sent do to complete it's tasks? | Nemucod would contact C2C servers and download DLL executable files that contain malwares |

1. What are your recommended mitigation strategies?  
     
    Answer:
   * 1. Train employees of the State of California to not open suspicious emails from unknown senders. If they find it suspicious, they can forward it to the CIRT team who can open it in a sandbox environment and verify.
     2. When identified, CIRT team can add SNORT rules to reject packets from this source IP
     3. If an employee has already opened the email, remove it from network and use latest antimalware signatures to uninstall the threat
     4. Update antivirus and antimalware signatures (like Windows defender, Malware bites) on all machines and run scans
     5. Build rules on Firewall to identify if any machine is phoning to identified C2C servers
2. List your third-party references.  
     
    Answer:

<https://www.certego.net/en/news/italian-spam-campaigns-using-js-nemucod-downloader/>

<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=JS/Nemucod>